



Seth Berman
Direct Line: (617) 439-2338
Fax: (617) 310-9338
E-mail: sberman@nutter.com

January 31, 2019

By FedEx

Attorney General Gordon MacDonald
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED

FEB 01 2019

CONSUMER PROTECTION

Re: Security Event Notice Provided for Aptus Health Inc.

Dear Attorney General MacDonald:

We represent Aptus Health Inc. (“Aptus Health”) with respect to a data security event involving the potential exposure of certain personal information described in more detail below.

The purpose of this letter is to provide your office with formal notice that Aptus Health has been a recent target of a business email compromise, which led to the criminal access of an Aptus Health email account. The affected email account contained spreadsheets detailing the names and social security numbers of Aptus Health’s employees, contractors, and others related to the company. For some of the affected individuals, the email account also contained the subjects’ bank account numbers, bank routing numbers, passport numbers, and/or addresses. The relevant email account did not include any customer data or health information.

After an extensive review of the available logs and other data, we have not been able to determine whether the attackers actually accessed the above-mentioned personal information or if they only accessed other information in the email account. However, in the interest of protecting the affected individuals, we are treating this incident as a data breach.

The Nature of the Breach

On or about December 13, 2018, Aptus Health became aware of evidence that suggested that, following a phishing attack, hackers had accessed an Outlook email account of a payroll manager in its Finance Department. This evidence came to light in part as a result of a then-ongoing investigation which had been instituted after evidence that a different Aptus Health email account had been compromised. After discovering the evidence that suggested that the payroll manager’s account had been accessed, Aptus Health worked with its outside vendor, Booz Allen Hamilton (“BAH”) to determine the nature and scope of the breach and whether any personally identifiable information (“PII”) had been in the impacted email account. BAH reviewed the available computer logs and other evidence to determine that the hackers had access to the email account during the period from approximately August 17, 2018 until approximately October 5, 2018. In January 2019, BAH determined that the relevant email

January 31, 2019

Page 2

account contained the PII of Aptus Health employees, contractors and others related to the company, but was unable to determine whether any of this PII was actually accessed by the hackers.

Steps Taken or Planned to be taken Related to the Security Event

In response to the breach, Aptus Health is working to improve security by implementing additional safeguards on its web server infrastructure and is taking steps to protect personal data from theft or criminal activity in the future. Immediately upon learning of the attack, Aptus Health required all users to change their passwords, and began implementing multi-factor authentication for all email logins. Aptus Health also implemented email notifications regarding suspicious activity; issued new laptops to certain users; quarantined several laptops while completing malware scans and reviewing patch and event logs; blacklisted credential harvesting IP's; upgraded firewalls; implemented monthly review of Office365 Cloud App Security; and enhanced email security by implementing a Sender Policy Framework (SPF), DomainKeys Identification Mail (DKIM) and Domain Message Authentication Reporting & Conformance (DMARC) to reduce the number of phishing emails that can enter the domain.

In addition, Aptus Health is offering identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide affected individuals with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help affected individuals resolve issues if their identity is compromised.

Aptus Health also notified the FBI of the incident immediately after it was discovered.

Number of New Hampshire Residents Affected

Eight New Hampshire residents were affected by the breach. Aptus Health anticipates mailing the notification letter to the affected individuals on January 31, 2019. A copy of the form notification letter is enclosed.

Very Truly Yours,



Seth Berman

SPB2:pjm
Enclosure



C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR, 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.myidcare.com/account-creation/protect>
Enrollment Code:
<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 31, 2019

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

This letter is written to inform you that on January 2, 2019, we discovered that a data breach of an Aptus Health email account implicated personal and confidential information. Some of the personal and confidential information contained in this email account related to you. We have learned that the breach occurred during the time period from August to October 2018. We do not have any indication that your specific information was actually accessed by the attackers or that it has been misused.

What Information Was Involved

The information included your <<variable data 1>>.

What We Are Doing

We are working to improve security by implementing additional safeguards and we are taking steps to protect personal data from theft or criminal activity in the future. To achieve these goals, we will be rolling out two-step authentication on all our accounts, among other increased security features.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is May 1, 2019.

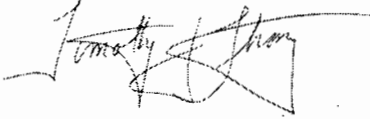
Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to <https://app.myidcare.com/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "Timothy J. Thompson". The signature is stylized and somewhat cursive, with a long horizontal line extending to the right.

Timothy J. Thompson
CEO
Aptus Health

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

In order to request a security freeze, you will need to provide the following information:

1. Your full name;
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identifiable card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: You can obtain information about steps you can take to avoid identity theft from the FTC or the Office of the Maryland Attorney General. Contact: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.